(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/92999 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/16467

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/579,910 26 May 2000 (26.05.2000) US

(71) Applicant: **CITRIX SYSTEMS, INC.** [US/US]; 6400 NW 6th Way, Fort Lauderdale, FL 33309 (US).

(72) Inventors: **OTWAY, David, John**; 12 Willis Road, Cambridge CB1 2AQ (GB). **BULL, John, Albert**; The Almshouses, Great Brington, Northampton NN7 4HY (GB).

(74) Agent: **RODRIGUEZ, Michael, A.**; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/92999 A2

(54) Title: SECURE EXCHANGE OF AN AUTHENTICATION TOKEN

(57) Abstract: A method and system for securely exchanging an authentication token. In one embodiment, the communication system includes a first transmitter in communication with a first receiver and a second transmitter in communication with a second receiver. A comparator is in communication with the first receiver and the second transmitter. An output device is in communication with the second receiver. The user transmits user information to the first receiver over a first communication channel. The first receiver receives this user information, and subsequently transmits a first verification message to the second receiver over a second communication channel. In response to the first verification message, the user sends a second verification message back to the first receiver over the first communication channel. The first receiver receives this first verification message and the comparator determines authenticity by comparing the first verification message transmitted over the second communication channel with the second verification message received over the first communication channel.

SECURE EXCHANGE OF AN AUTHENTICATION TOKEN

FIELD OF THE INVENTION

The invention relates in general to secure communication systems and more specifically systems for securely exchanging an authentication token.

BACKGROUND OF THE INVENTION

Security of communication systems on a network is a major obstacle to transmission of private data faced by companies and individuals alike. Most businesses and individuals place great reliance on the privacy of information, and therefore unauthorized tampering with or theft of information could have serious financial and safety effects. A fixed user password is not a secure means of authentication because it is rarely changed and easily guessed. Once an unauthorized user determines a valid user password, the unauthorized user has access to all information in the user's computer account.

To accomplish a secure exchange of information between two systems, a hardware authentication token can be employed. A hardware authentication token is a specialized device that gives the user a one-time password or method that the user inputs into the server expecting such input. One such token is the SecurID™ token, developed

by RSA Security in Bedford, MA. The SecurID™ system includes a SecurID™ token generator which the user carries, and an access control module (ACM) which is connected to the computer to which the user wants access. The SecurID™ token generator is a smart card that is time synchronized to the ACM. The SecurID™ token generator has a display for a sequence of random digits corresponding to the random digits generated by the ACM. The sequence of random digits is unique for each SecurID™ token generator, and the random number displayed changes after a certain time limit. To obtain access to the server, the user inputs the random number displayed on the token generator. If the number entered by the user into the server matches the response expected by the server, the server concludes that the user is authentic.

Due to the global electronic world in which we live, our lives are surrounded by electronic devices. People travel with cellular phones, a personal digital assistant (PDA), a laptop, etc. to be connected to people and other devices. Because of the number of devices people travel with already, people are becoming more likely to forget one of these devices or leave one of these devices unattended. Hardware authentication token generators such as the SecurID™ are yet another item for people to remember and carry. Furthermore, the hardware authentication token generators add an additional cost to the user. Therefore, it is desirable to produce an equivalent authentication method for

exchanging information that does not require another item to travel with or to provide an additional cost to the user.

SUMMARY OF THE INVENTION

The invention relates to a communication system that securely exchanges an authentication token. In one embodiment, the communication system includes a first transmitter in communication with a first receiver and a second transmitter in communication with a second receiver. A comparator is in communication with the first receiver and the second transmitter. An output device is in communication with the second receiver.

The user transmits user information to the first receiver over a first communication channel. The first receiver receives this user information, and subsequently transmits a first verification message to the second receiver over a second communication channel. In response to the first verification message, the user sends a second verification message back to the first receiver over the first communication channel. The first receiver receives this second verification message and the comparator determines authenticity by comparing the first verification message transmitted over the second communication channel with the second verification message received over the

first communication channel.

DESCRIPTION OF THE DRAWINGS

The aspects of the invention presented above and many of the accompanying advantages of the present invention will become better understood by referring to the included drawings, which show a system according to the preferred embodiment of the invention and in which:

FIG. 1 is a block diagram of an embodiment of the communications system of this invention to securely exchange an authentication token.

FIG. 2 is a flow chart illustrating an embodiment of the steps for executing an embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In brief overview, the communication system in one embodiment includes a first computer, which may be referred to as a client computer, in communication with a second computer, which may be referred to as a server computer. The server computer is in turn in communication with a verifier, which in one embodiment is a mobile phone.

A user wishing access to the server logs onto the client computer. In one

embodiment, the client computer then sends the user's user information to the server. The server uses the user information to find which verifier or mobile phone is associated with the user. The server then generates a datum or code which it transmits to the mobile phone associated with the user. The mobile phone displays the datum to the user who then enters the datum into the client computer. The client computer in turn sends the datum back to the server which compares the datum sent to the verifier with the datum received from the client computer. If the two data match, the server then permits access by the user to the server.

Referring to FIG. 1, the first computer, or client 10, is in communication with the second computer, or server 30, over a communication channel 15. Communication channel 15 may be a secure communication channel. Server 30 is in turn in communication with the verifier 50 over a communication channel 40. Communication channel 40 may be a secure communication channel. The verifier 50, which in one embodiment is a mobile phone, displays to or communicates with the user. The user enters the information he or she received from the display into the client 10. In this diagram, this is depicted as the verifier being in communication with the client 10 over a communication channel 55.

In another embodiment, the verifier 50 is a non-mobile telephone with a confidential phone line to the server 30. In yet another embodiment, the verifier 50 is a PDA capable of receiving message 35 over a confidential channel. In another embodiment, the verifier 50 is a laptop or beeper capable of communicating with server 30 over a confidential communication channel.

More specifically, message 20, sent from client 10 to server 30, in one embodiment includes a user's name with which the server 30 recognizes the user and begins the process by which the server 30 allows access to the server 30 by the user. In another embodiment, message 20 is any code or method that server 30 accepts as a way to access the user's account on server 30. In yet another embodiment, message 20 is biometric information or a voice message that server 30 will recognize as user information for that particular user. Once the user information from message 20 is received by server 30 over communication channel 15, server 30 determines a method to communicate with the verifier 50. In one embodiment, the method includes selecting the communication channel 40. Once such a method is determined, server 30 transmits a verification message 35 to the verifier 50.

In one embodiment, the verifier 50 is a communication device such as a Global

System for Mobile (GSM) communications telephone. GSM is a communication standard for mobile telephones and provides a confidential communication channel between a caller and the GSM telephone. The server 30 sends a message 35 to the mobile phone via a Short Message Service (SMS) message. The GSM cellular phone supports the SMS message, as defined within the GSM digital phone standard. The advantage of SMS messages are that they can be sent and received simultaneously with GSM voice, data, and fax calls. By using this advantage, the GSM mobile phone will receive a SMS message while simultaneously being engaged on a call, and so the mobile phone will permit conversation at the same time as connecting a laptop to a server and authenticating it.

In one embodiment, the server 30 retrieves from its computer memory a mobile cellular telephone number for the user that can be used to communicate with the verifier 50. Server 30 then generates the message 35 and transmits the message 35 to the verifier 50. In another embodiment, the message 35 generated by the server 30 is either mathematically manipulated or encrypted prior to the transmission to the verifier 50.

In one embodiment, the contents of message 35 received by the verifier 50 are produced on the mobile cellular phone display. Similarly, in another embodiment, the

output of message 35 is accomplished by a voice message, an email, or any other method to report the contents of message 35 to the user. Although in this embodiment the verifier 50 is a cellular phone, any device which is capable of communications with server 30 can be used.

As shown in FIG. 1, in one embodiment the verifier 50 displays the message 35 to the user. The user types in this information over communication channel 55 along with the user's password for the server 30 into the client 10. In another embodiment, instead of displaying message 35 to the user and having the user type in this information to the client 10, the verifier 50 directly transmits another message 60 with the verification information 35 to the client 10 over a direct electrical, wireless or optical communication channel 55. The client 10 receives message 60 and automatically sends this information to server 30 through a message 65 over communication channel 15.

In one embodiment, the server 30 receives a message 65, extracts the verification information 35, and compares the verification information with the verification message 35 it sent to the verifier 50. The server 30 accepts the user as authentic if the two messages match. If the two messages do not match, the user is not accepted and classified as unauthentic. It should be understood that any combination of messages

may be used as long as the server 30 can compare what it receives from the client 10 to what it sent to the verifier 50.

The operation of the present invention in one embodiment is shown in FIG. 2. The user first transmits his username (101) to the server 30 by way of the client 10. The server 30 determines the method to communicate with the verifier 50 by accessing stored information (102). Subsequently, the server generates a random number (103). After the generation of the random number, the server concurrently transmits the random number to the verifier 50 and starts a timeout period in which the server must receive a verification message back from the client 10 (104).

The verifier 50 then receives the random number and displays it for the user to read (105). The user types this random number along with the user's password to the server 30 into the client 10 (106). The client 10 passes this message 65 along to the server 30 for verification (107). The server receives the message 65 (108) and determines if the received message 65 was received within the timeout period (109). If it was not received in the required time, the server concludes that the user is not authentic (110). If the message was received within the timeout period, the server compares the received random number to the stored random number it sent and also

verifies the user's password (111). If these do not match (112), the server concludes that the user is not authentic (113). If these do match (112), the server determines that the user is authentic (114).

While one embodiment of the invention has been illustrated, it will be appreciated that various changes can be made without parting from the scope of the invention. For example, the security between client 10 and server 30 is increased in one embodiment by using client 10 to encrypt the user's password using the random number before transmitting it to server 30. Additionally, communication channel 15 is confidential in another embodiment.

The ultimate goal of the present invention is to supply the server 30 with any number or message that it is expecting in response to the transmitted message. So in one embodiment, the mathematical manipulation of the verification message 35 is computed mentally by the user. For example, the user adds one to the random number received from the server 30 and types this modified number into the client 10. As long as the server 30 is expecting this manipulated message in response to the transmitted message, the user will be deemed authentic.

It will be appreciated that the embodiments described above are merely examples

of the invention and that other embodiments incorporating variations therein are considered to fall within the scope of the invention. In view of the foregoing, what I claim is:

1. A method for verifying a user to a first computer comprising the steps of:

transmitting user information on a first communication channel;

receiving said user information by said first computer;

transmitting a first verification message to said user on a second communication channel in response to said user information;

receiving said first verification message by said user;

transmitting a second verification message by said user to said first computer over said first communication channel in response to said first verification message;

receiving said second verification message by said first computer on said first communication channel; and

comparing by said first computer said first verification message transmitted over said second communication channel with said second verification message received over said first communication channel.

2. The method of claim 1, wherein said first verification message is a random number

generated by said first computer.

3. The method of claim 1, wherein said second verification message comprises said first verification message.

4. The method of claim 3, wherein said second verification message is a mathematical function of said first verification message.

5. The method of claim 1, wherein said second verification message further comprises said user's password to said first computer.

6. The method of claim1, wherein said first communication channel is a cellular communication channel.

7. The method of claim 1, wherein said second communication channel is a cellular communication channel.

8. The method of claim 1, wherein said first communication channel is a confidential communication channel.

9. The method of claim 1, wherein said second communication channel is a confidential communication channel.

10. The method of claim 1, wherein transmitting said first verification message further comprises the steps of starting a clock by said first computer and measuring a timeout period by said clock wherein said timeout period defines the period of time during

which said second verification message must be received by said first computer.

11. A system for securely exchanging an authentication token comprising:

a first transmitter;

a first receiver in communication with said first transmitter;

a second transmitter;

a second receiver in communication with said second transmitter;

a comparator in communication with said first receiver and said second transmitter; and

an output device in communication with said second receiver,

wherein said second transmitter transmits a first verification message to said second receiver over a second communication channel,

wherein said first transmitter transmits a second verification message to said first receiver over a first communication channel, and

wherein said comparator compares said first and said second verification messages.

12. The system of claim 11, wherein said second communication channel is a cellular communication channel.

13. The system of claim 11, wherein said first communication channel is a cellular communication channel.

14. The system of claim 11, wherein said first communication channel is a confidential communication channel.

15. The system of claim 11, wherein said second communication channel is a confidential communication channel.

16. The system of claim 11, wherein said comparator determines whether said second verification message transmitted by said first transmitter comprises said first verification message transmitted by said second transmitter.

17. The system of claim 11, wherein said comparator determines whether said second verification message transmitted by said first transmitter comprises a password associated with a user.

18. The system of claim 11, wherein said output device transmits said second verification message.

19. The system of claim 11, wherein said system further comprises a first input device in communication with said first transmitter and said output device.

20. The system of claim 19, wherein said output device is in communication with said first input device over a communication channel.

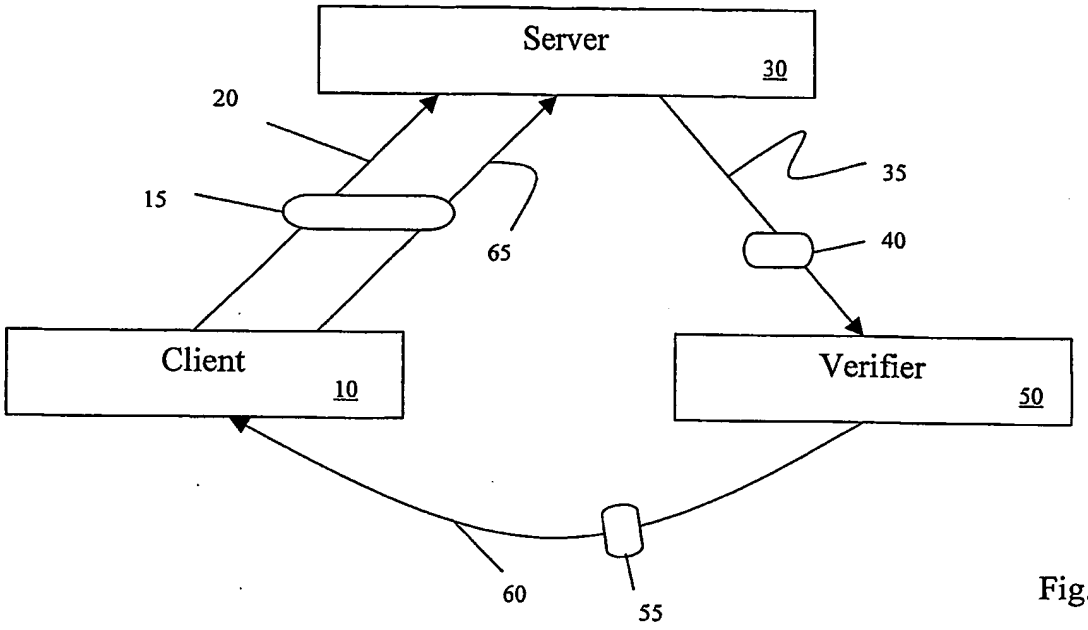

Fig. 1

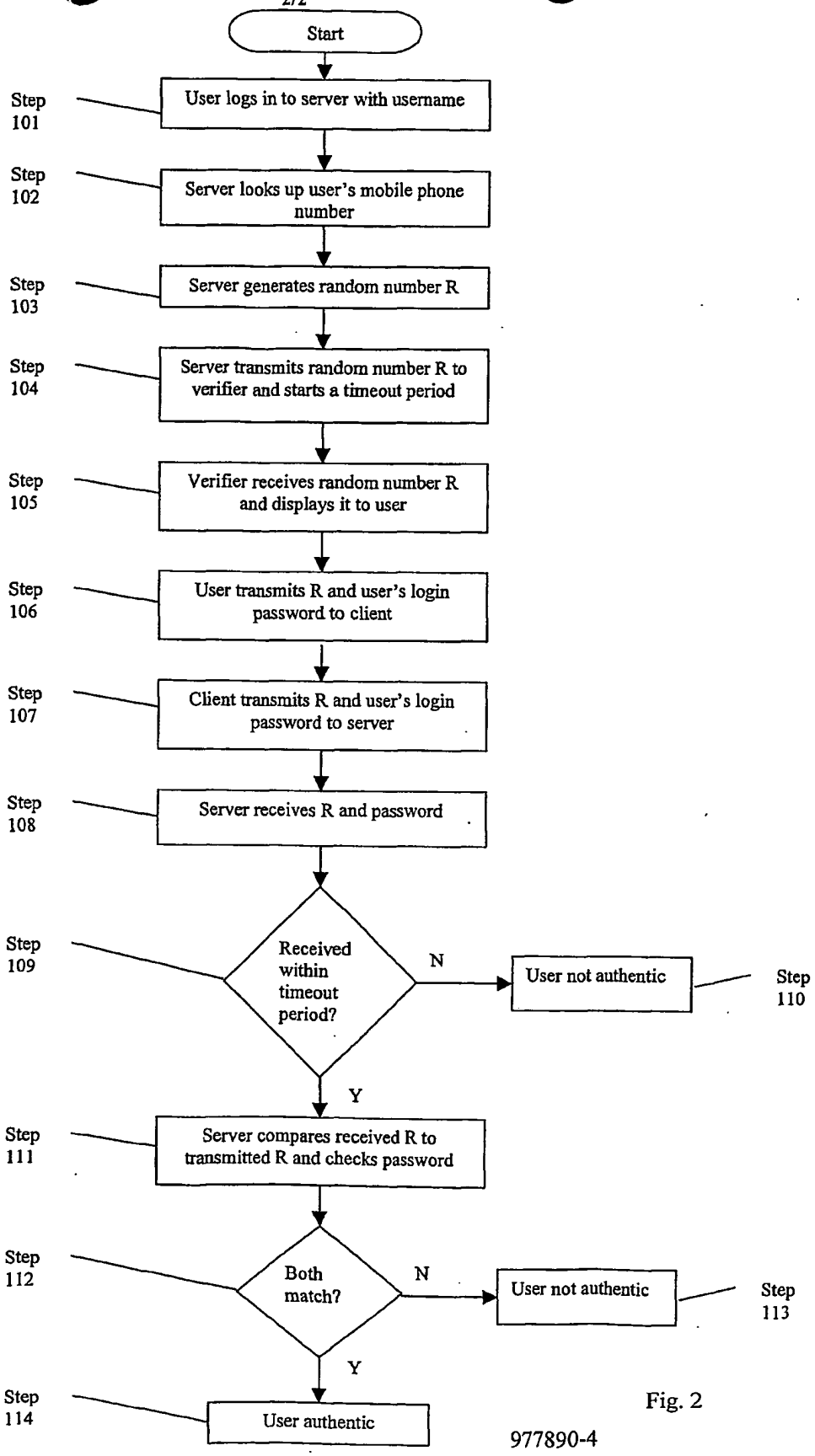

Fig. 2

977890-4